Dr. Hans-Jaochim Müschenborn 16101

Protection of security critical data in networks

Claims

1. Network system comprising at least one central unit ZE, at least one service unit SE physically connected with ZE and an arbitrary number of physically with ZE connected peripheral units PE1..n, wherein ZE executes at least one thread - called central process or thread -, SE executes at least one thread S - called critical service -, the peripheral or central units execute an arbitrary number of peripheral threads and wherein at least one critical service can build-up or accept at least one standing logical bidirectional communication connection to or from at least one central process, and wherein on top of said connection(s) between the critical service(s) and the central process(es) no further connections can be build-up or accepted by threads running on SE, and wherein direct logical communication connections between peripheral threads running on a peripheral or a central unit and ZE can be established, such that data stored on SE is accessible for the central processes only via a critical service and for the peripheral processes only via a central process and a critical service.

2. Network system according to claim 1 wherein at least one central process assigns at least one logical identification to at least one connection to a critical service connected to said central process, such that a peripheral thread is able only with the knowledge of said logical identification(s) to communicate indirectly via said central process with at least one member out of a group of critical services, which group is uniquely identified by said logical identification(s).

3. Network system according to one of the claims 1 or 2 comprising at least two segments N1 and N2, at least one central unit ZE physically connected with each of the segments N1 and N2, at least one service unit SE in segment N1 and physically connected with ZE and an arbitrary number of peripheral units PE1..n physically connected with ZE wherein direct logical communication connections between peripheral threads running on a peripheral unit within N1 or N2 or a central unit and ZE can be established, whereby said central unit(s) are able to build-up or accept direct logical connections to or from units in N1 or N2, and whereby units in N1 cannot establish direct logical connections to units in N2 with the exception of said central process(es), and whereby units in N2 cannot establish direct logical connections to units in N1 with the exception of said central process(es), and whereby units in N1 cannot accept direct logical connections from units in N2 with the exception of said central process(es), and whereby units in N2 cannot accept direct logical connections from units in N1 with the exception of said central process(es).

4. Network system according to one of claims 1 to 3, wherein the central unit ZE stores authorization data AD and wherein at least one peripheral thread after connecting to the central process Z on ZE transmits access data to Z, and wherein Z checks the access rights of the peripheral process by checking said access data against said authentization data AD, and wherein Z terminates the connection to said peripheral process if the result of said check of said access rights is negative.

5. Network system according to one of claims 1 to 3, wherein at least one Unit AE directly or indirectly physically connected with central unit ZE stores authorization data AD and wherein AE executes at least one authorization thread AS able to build-up or accept a standing logical connection to or from Z, and wherein at least one peripheral thread after build-up of the connection to central process Z sends Z access data, and wherein Z receives said access data and forwards said access data to AS, and wherein AS receives said access data,

checks the access rights of said peripheral process by checking said access data against said authorization data AD and transmits the result of said check of said access rights to Z, and wherein Z terminates the connection to said peripheral process if the result of said check of said access rights is negative.

6. Network system according to claim 1, wherein at least one central unit executes at least one thread - called logon process or thread - providing at all times at least one open connection endpoint identified by a fix local identification, and wherein no central process(es) provide open connection endpoints without prior trigger from said logon process, and wherein at least one peripheral thread to connect to a central process(es) establishes first a connection to said logon process, and wherein said logon process via an arbitrary inter-thread- or interprocess communication medium triggers at least one central process to open a new connection endpoint, and wherein at least one of the triggered central processes opens for a predefined time interval a new connection endpoint with a local identification known to said peripheral thread, and wherein said peripheral thread connects to at least one of said opened connection endpoint(s) of at least one central process within said predefined time interval, and wherein all triggered central processes close all opened connection endpoints to which said peripheral process did not connect to within said predefined time interval.

7. Network system according to claim 6 wherein the communication medium between at least one logon process and at least one central process is a standing logical connection.

8. Network system according to one of the claims 6 or 7 wherein at least one peripheral thread transmits to the logon process additional access data, and wherein the logon process checks the access rights of said peripheral process by checking said access data against predefined authorization data,

SubA3

and wherein said logon process triggers at least one central process to open a new connection endpoint only if said authorization check returns a positive result.

9. Network system according to claim 6 wherein at least one unit AE stores authorization data, and wherein each of the unit(s) AE is(are) physically connected to at least one central unit, and wherein each of the unit(s) AE executes an authorization service AS, which service is able to establish or to accept standing logical connections to or from at least one logon process and to or from at least one central process, and wherein a peripheral thread after connecting to a logon process sends said logon process its access data, and wherein said logon process forwards each connection request of a peripheral thread together with said access data to said authorization service AS, and wherein said authorization service AS checks the access rights of said peripheral thread by checking said access data against authorization data AD and in case of a positive result triggers at least one central process to open a new connection endpoint, and wherein at least one of the triggered central processes provides for a predefined time interval a new open connection endpoint with a local identification known to said peripheral thread, and wherein said peripheral thread connects to at least one of said temporarily opened connection endpoint(s) within said predefined time interval, and wherein all central process(es) close all temporarily opened connection endpoints to which said peripheral thread did not connect to within said predefined time interval.

SubA4

10. Network system according to one of the claims 6 to 9 wherein at least one peripheral thread does not know the local identification of at least one temporarily opened connection endpoint by at least one central process, and wherein said peripheral thread receives said local identification from at least one logon process.

11. Network system according to claim 10 wherein at least one logon process generates at least one local identification of at least one connection endpoint to be provided by at least one of the central processes and transmits said generated local identification during connection build-up to at least one peripheral thread and to at least one central process providing a new temporarily opened connection endpoint with said local identification.

12. Network system according to claim 10 wherein at least one central process generates at least one local identification of at least one connection endpoint to be provided by at least one of the central processes and transmits said generated local identification during connection build-up via at least one logon process to at least one peripheral thread.

Sub A5

13. Network system according to claims 9 and 10 wherein at least one authorization service generates at least one local identification of at least one connection endpoint to be provided by at least one of the central processes and transmits said generated local identification during connection build-up via at least one logon process to at least one peripheral thread and to at least one central process providing at least one temporarily open connection endpoint with said generated local identification.

14. Network system according to one of claims 9 to 13 wherein at least one local identification of at least one temporarily opened connection endpoint of at least one central process is generated randomly or pseudo-randomly.

15. Network system according to one of claims 9 to 14 wherein at least one local identification of at least one temporarily opened connection endpoint of at least one central process is transmitted in at least one encrypted message.

Sub A5

16. Network system according to one of the claims 6 to 15 wherein at least one peripheral thread does not know the physical address of the network interface of at least one target central unit, and wherein said peripheral thread receives from at least one logon process the physical address of at least one network interface of at least one central unit executing at least one central process providing at least one temporarily open connection endpoint.

17. Network system according to claim 16 wherein at least one logon process selects at least one central process Z1 providing at least one temporarily open connection endpoint and transmits the physical address of the network interface of the central unit executing Z1 to at least one peripheral thread during connection build-up.

18. Network system according to claim 16 wherein at least one central process selects at least one central process Z1 providing at least one temporarily open connection endpoint and transmits via at least one logon process the physical address of the network interface of the central unit executing Z1 to at least one peripheral thread during connection build-up.

Sub A6 Cont

19. Network system according to one of the claims 9 to 16 wherein at least one authorization service selects at least one central process Z1 providing at least one temporarily open connection endpoint and transmits via at least one logon process the physical address of the network interface of the central unit executing Z1 to at least one peripheral thread during connection build-up.

20. Network system according to one of the claims 16 to 19 wherein at least one central process is selected randomly or pseudo-randomly.

Sub A6 Cont

21. Network system according to one of the claims 16 to 20 wherein the physical address of at least one network interface of at least one central unit running at least one central process providing at least one temporarily open connection endpoint is transmitted in encrypted form.

22. Network system according to one of the previous claims wherein at least one service builds-up or accepts at least one standing logical connection to or from at least two central processes, and wherein said service provides on at least two of its connections different protocols.

23. Network system according to one of the previous claims wherein at least one of the protocols of at least one service can be activated during operation.

24. Network system according to one of the previous claims wherein at least one of the protocols of at least one service can be deactivated during operation.

25. Network system according to one of the claims 23 or 24 wherein the activation or deactivation of at least one protocol of at least one service is controlled by at least one function of at least one protocol of said service.

26. Network system according to one of the previous claims wherein at least one function of at least one protocol of at least one service can be activated during operation.

27. Network system according to one of the previous claims wherein at least one function of at least one protocol of at least one service can be deactivated during operation.

28. Network system according to one of the claims 26 or 27 wherein the activation or deactivation of at least one function of at least one protocol of at least one service is controlled by at least one function of at least one protocol of said service.

29. Network system according to one of the previous claims wherein at least one protocol of at least one service can be loaded into the addressable memory space of said service during operation.

30. Network system according to one of the previous claims wherein at least one protocol of at least one service can be removed from the addressable memory space of said service during operation, such that all functions of said removed protocol can only be called again after said protocol has been loaded again into the addressable memory space of said service.

31. Network system according to one of the claims 29 or 30 wherein the loading or removal of at least one protocol of at least one service is controlled by at least one function of at least one protocol of said service.

32. Network system according to one of the previous claims wherein at least one function of at least one protocol of at least one service can be loaded into the addressable memory space of said service during operation.

33. Network system according to one of the previous claims wherein at least one function of at least one protocol of at least one service can be removed from the addressable memory space of said service during operation, such that said removed function can only be called again after said removed function has been loaded again into the addressable memory space of said service.

Sub A6

34. Network system according to one of the claims 32 or 33 wherein the loading or removal of at least one function of at least one protocol of at least one service is controlled by at least one function of at least one protocol of said service.

35. Network system according to claim 10 wherein the choice of a central process depends on the authorization of said peripheral thread, or the number of peripheral threads connected to each eligible central process, or on the load of each eligible central process, or on the system demands of said peripheral thread, or on the quality and speed of the connection between said peripheral thread and the logon central process or each eligible central process, or on the geographical position(s) of the eligible central unit(s) or the peripheral unit executing said peripheral thread, or on the network topological location(s) of the peripheral and eligible central unit(s), or on the system topological location(s) of the peripheral thread or the eligible central process(es).

36. Network system according to claim 16 wherein the choice of a central unit executing an eligible central process - called eligible unit - depends on the authorization of said peripheral thread, or the number of peripheral threads connected to each eligible central process or central unit, or on the load of each eligible central unit, or on the system demands of said peripheral thread, or on the quality and speed of the connection between each eligible central process and said peripheral thread, or on the geographical position(s) of the eligible central unit(s) or the peripheral unit executing said peripheral thread, or on the network topological location(s) of the peripheral and eligible central unit(s), or on the system topological location(s) of the peripheral thread or the eligible central unit(s) running eligible central process(es).